International Journal of Engineering, Management and Humanities (IJEMH)
Volume 4, Issue 3, May-June, 2023 pp: 166-169 www.ijemh.com

Honeypot Architecture for Network Threat Quantification

Harsh Raj[1], Pranshu Pandey[2], Shashank Shekhar[3], Chandrasekhara N[4]
[1,2,3,4] *Department of Electronics & Communication Engineering, Dayananda Sagar College of Engineering, Karnataka, India.*

Date of Submission: 24-05-2023 Date of Acceptance: 05-06-2023

Abstract - In today's interconnected world, computer networks have become increasingly vital. However, this reliance also brings about a surge in security challenges. Each day, new threats and vulnerabilities are discovered, affecting both individuals and companies in various ways, such as privacy breaches and financial losses. To understand and address these issues, it is crucial for researchers and security analysts to monitor network activity. Honeypots were introduced as a means to monitor unused IP spaces and gather information about attackers. However, deploying and managing honeypots in large organizations can be costly and complex. To tackle this, a novel hybrid honeypot architecture is proposed, utilizing a Decision Engine and Redirection Engine to automatically filter attacks and reduce the size of data collection. Additionally, the architecture integrates network flows collected at the production network's border, providing a comprehensive view of internal and external communications and enabling accurate threat assessments.

Keywords - *Honeypot, Suspicious Packet flow, Malware, Vulnerability Management, Security Framework*

I. Introduction

The reliance on network resources is rapidly increasing, leading to larger and more complex network infrastructures. Each day, new threats and vulnerabilities are discovered, leaving computer systems far from being truly secure.

Shockingly, after COVID-19 pandemic when every sector moved towards digitalization, vendors, researchers, and independent experts disclosed a staggering number of vulnerabilities. What's more alarming is that between 8% and 16% of these vulnerabilities were immediately exploited by malicious programs upon their disclosure. The consequences of these security breaches have critical implications, impacting both users and companies in terms of privacy issues and financial losses. In response to these concerns, network operators and security researchers have developed and implemented various solutions. The primary objectives of these solutions are two- fold: first, to monitor network activity, and second, to protect network assets. Monitoring network activity allows researchers to gain valuable insights into the different types of threats that exist. By collecting and analyzing data, researchers can better understand and quantify malicious activities, contributing to an improved understanding of the security landscape. This framework is built upon a flexible hybrid honeypot architecture, seamlessly integrated with the organization's network infrastructure through the utilization of network flows. The hybrid honeypot architecture serves as a central component of the framework, offering scalability and flexibility in monitoring and capturing malicious activities. By combining various techniques and technologies, this architecture enables efficient data collection, analysis, and response to potential threats. [1] The integration of honeypots with the organization's network through network flows ensures a comprehensive and accurate measurement of malicious activities

Overall, this dissertation aims to address the pressing need for better measurement and understanding of malicious threats within organizational networks. The proposed framework, based on the innovative hybrid honeypot architecture, promises to provide security practitioners with enhanced capabilities to monitor, detect, and mitigate potential security breaches, ultimately leading to improved network security and resilience.

II. Reference Study

In this paper [2] The research signifies that Over the years, honeypots have proven to be highly effective in identifying attackers and thwarting various types of large-scale cyber- attacks. Despite being nearly three decades since their discovery, more than 80% of companies continue to rely on honeypots due to their intrusion detection capabilities and low false positive rates. [3] This paper examines different methods of implementing honeypot networks and provides insights into the challenges associated with these techniques, along with their corresponding solutions. Furthermore, it delves into the most preferred solution among the techniques discussed in the paper. The frequency of internet attacks is steadily increasing, posing a significant threat to our security systems. To mitigate this risk, it is crucial to have a robust security system capable of detecting and blocking zero-day attacks. [4] This paper proposes a honeypot-based model for an intrusion detection system (IDS) that aims to gather the most valuable data about attackers. Extensive testing was conducted to assess the capabilities and limitations of honeypots, leading to the identification of areas that require improvement. Moving forward, the primary goal is to harness this emerging trend for proactive measures, enabling early prevention and ensuring the protection of our security systems against potential threats that may arise unexpectedly.

By taking preemptive action, we aim to safeguard our infrastructure and mitigate any potential harm before it can materialize and cause damage to the production server and also keep the production server up and running for the legitimate users who are authorized to access the resources.

III. Materials and Methods

By identifying and redirecting users displaying abnormal behavior to a honeypot server, we can effectively analyze the tactics and techniques employed by attackers to breach our system. This analysis enables us to strengthen the security infrastructure of our own server, safeguarding it against future attacks. [5] The detection of unusual user behavior serves as an early warning system, flagging potentially malicious activities. By redirecting these users to a honeypot server, we create a controlled environment for further investigation. This allows us to closely examine the type of attack and the methodologies employed by the attackers. Analyzing the attack within the honeypot server provides valuable insights into the attacker's tactics, tools, and intentions. This information is then used to enhance the security measures implemented in our own server. By understanding the vulnerabilities exploited by the attackers, we can proactively address and mitigate these weaknesses, effectively fortifying our security infrastructure. The data collected from honeypot server analysis offers a deeper understanding of emerging threats, helping us develop robust countermeasures and strengthen our defenses. It enables us to stay one step ahead of potential attackers and ensure the integrity, confidentiality, and availability of our system. Ultimately, [6] by redirecting suspicious users to a honeypot server and leveraging the analysis of attacks, we can bolster the security of our own server, minimizing the risk of successful intrusions and maintaining a resilient and protected environment.

3.1 **Tracing the IP Address:** When encountering suspicious packets or requests that aim to harm or disrupt the server, making it inaccessible for legitimate users, these malicious packets will be intercepted and processed by a honeypot. The honeypot will diligently record the IP addresses and location information of the attackers, providing valuable data for further analysis and investigation.

3.2 **Capturing the System's Image:** The honeypot architecture is designed to handle suspicious packets or requests that aim to damage or disrupt the server, making it unavailable for legitimate users. It captures screenshots of the attacker's system, allowing for later analysis and tracing of their exact activities. These screenshots provide valuable insights into the nature of the attack and help identify potential vulnerabilities. [7] By studying the captured images, organizations can strengthen their security measures and fortify their systems against similar attacks in the future. The honeypot architecture, combined with the analysis of attacker system screenshots, enhances server security and safeguards the server's availability for legitimate users.

3.3 Logging Input Data and Determining the type of Vulnerability: Automatically logging data related to the observed fields, such as SQL injection or cross-site scripting, it helps determine the type of vulnerability being exploited. This information is crucial in strengthening the security infrastructure and implementing appropriate countermeasures. The honeypot architecture enables security teams to gain insights into emerging threats and attack techniques, allowing them to continuously improve the system's defense mechanisms. [6] By actively engaging with suspicious packets, it helps identify weaknesses and patch vulnerabilities, ensuring the server remains secure and accessible for legitimate users. Ultimately, the honeypot architecture plays a vital role in proactively protecting the server and hardening the security infrastructure against potential attacks.

3.4 Block Diagram

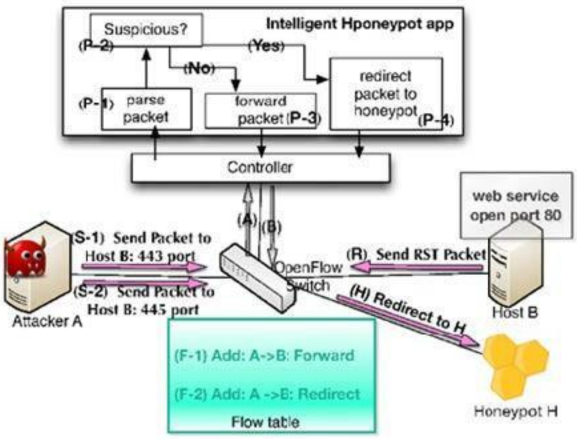


Figure 1

IV. Results

The following results are from the simulation of the Honeypot on Linux OS. The result shows the prevention of original server from attacker with the use of Honeypot Server.

4.1. Honeypot Server

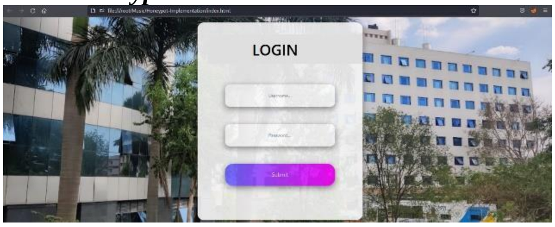
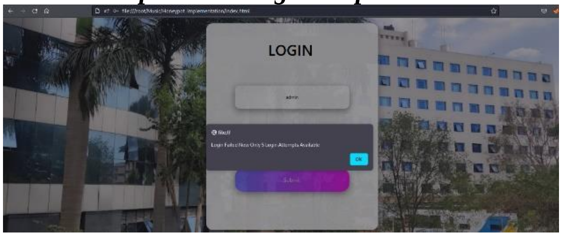


Figure 2

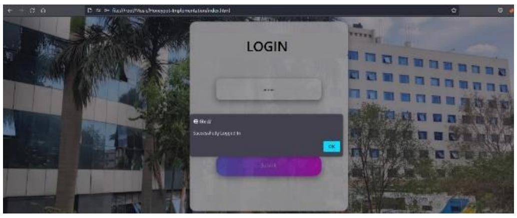
4.2. Attempt Remaining Prompt



file://
Login Failed Now Only 5 Login Attempts Available

Figure 3

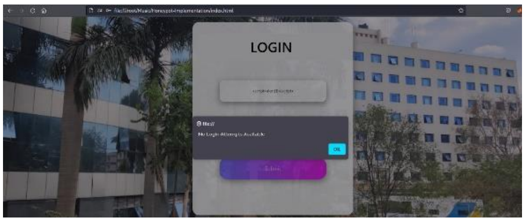
4.3. Successful Login Prompt



file://
Successfully Logged In

Figure 4

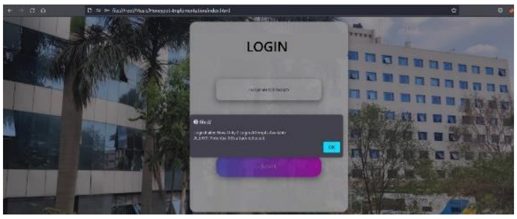
4.4. Login Attempts Exhausted



file://
No Login Attempts Available

Figure 5

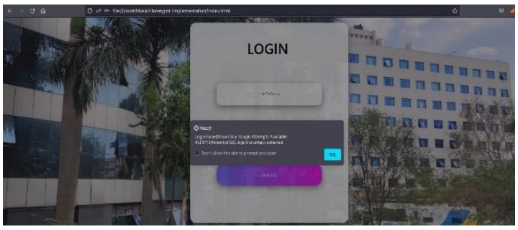
4.5. XSS Attack Detected



file://
Login Failed Now Only 2 Login Attempts Available
ALERT! Potential XSS attack detected

Figure 6

4.6. SQL Injection Attack Detected



file://
Login Failed Now Only 1 Login Attempts Available
ALERT! Potential SQL injection attack detected
□ Don't allow this site to prompt you again

Figure 7

V. Conclusion

In this paper, we have presented our work, Design and Implementation of Honeypot whose utilization can effectively safeguard the production server by thwarting any form of attack. This ensures that authorized users are never denied access to the resources they are entitled to. By diverting malicious activities towards the honeypot server, the production server remains shielded, allowing legitimate users to seamlessly utilize its resources without disruption. The honeypot server acts as a decoy, enticing attackers and diverting their attention away from the actual production server. It lures potential threats into a controlled environment, where their actions can be monitored and analyzed without posing a risk to the legitimate users or the production server itself. Through this proactive approach, the honeypot server serves as an additional layer of defense, detecting and deterring attackers before they can compromise the production server. Our Honeypot server not only prevents the attacker from exploiting vulnerabilities but also identifies which type of attack is being done. This enhances the overall security posture and ensures a reliable and uninterrupted experience for authorized users. By effectively isolating and containing malicious activities within the honeypot server, organizations can maintain the integrity and availability of their production resources, preventing unauthorized access and minimizing the impact of potential attacks.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Funding Statement

This research received no external funding

Acknowledgments

We'd like to express our heartfelt appreciation to Dr. T C Manjunath, the Head of the Department of Electronics and Communication Engineering at Dayananda Sagar College of Engineering, Bangalore and Dr. B G Prasad, the Principal of Dayananda Sagar College of Engineering, Bangalore for providing us with an opportunity for carrying out this research along with the necessary resources. Their unwavering support has been instrumental in the successful completion of this endeavor.

References

[1]. T. Sethi and R. Mathew, "A Study on Advancement in Honeypot based Network Security Model," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV).

[2]. F. R. Hariawan and S. U. Sunaringtyas, "Design an Intrusion Detection System, Multiple Honeypot and Packet Analyzer Using Raspberry Pi 4 for Home Network," 2021 17th International Conference on Quality in Research (QIR): International Symposium on Electrical and Computer Engineering

[3]. N. Bhagat and B. Arora, "Intrusion Detection Using Honeypots," 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC).

[4]. J. R. Kondra, S. K. Bharti, S. K. Mishra and K. S. Babu, "Honeypot-based intrusion detection system: A performance analysis," 2019 3rd International Conference on Computing for Sustainable Global Development (INDIACom).

[5]. M. Roesch, “Snort–lightweight intrusion detection for networks.”

[6]. C. Seifert and N.Z.H. Alliance, “Malicious SSH Login Attempts,” Adresse Internet

[7]. S. Small, J. Mason, F. Monrose, N. Provos, and A. Stubblefield, “To catch a predator: A natural language approach for eliciting malicious payloads.”